

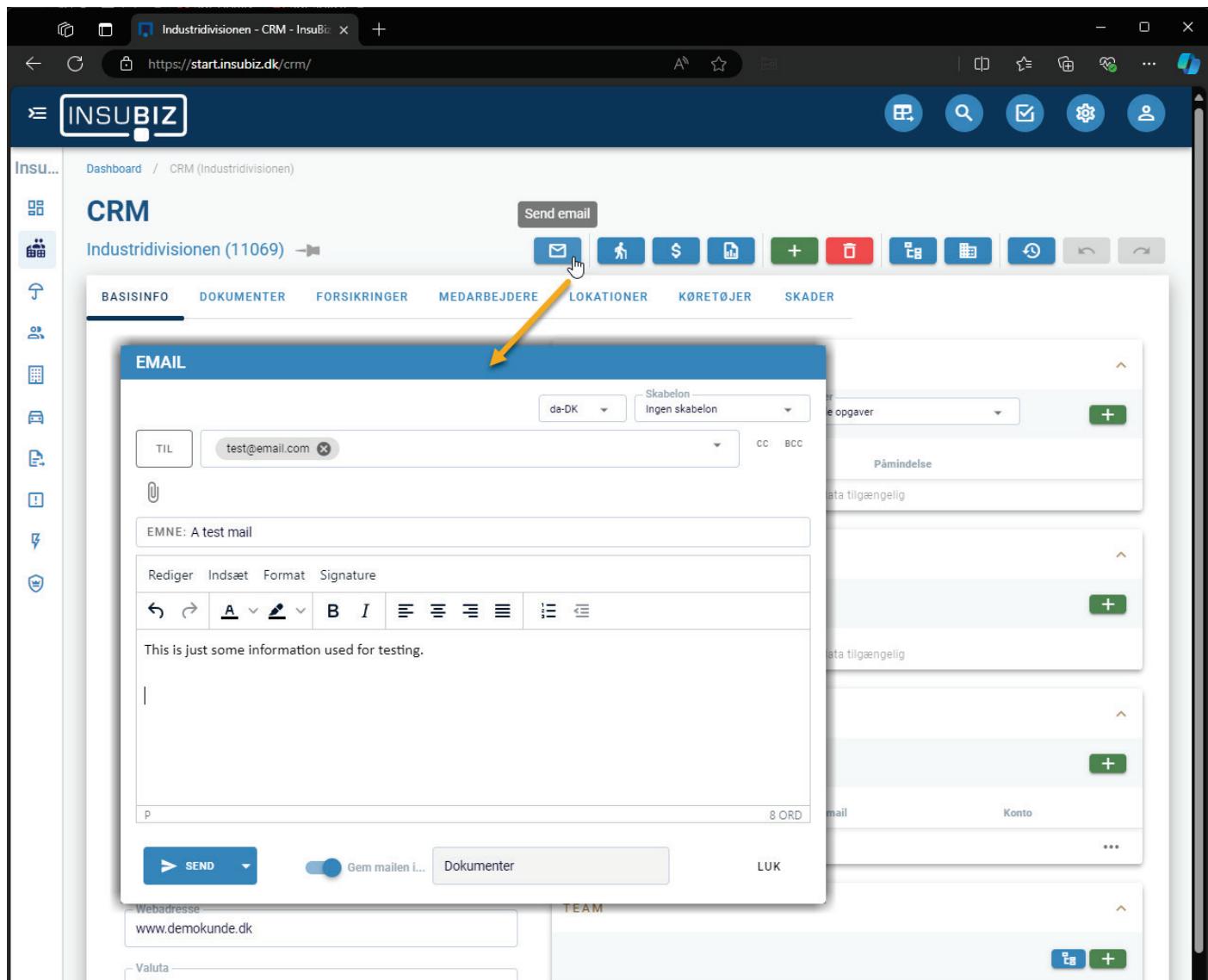
Contents

App description	2
Authentication	2
Security and permissions	3
Required permissions	3
Permission details	4
Permission approval and admin consent	6
Admin consent after user request	7
Admin consent using MS identity platform URL.....	11
Review the permissions in the Enterprise Application.....	13
Configuring the InsuBiz Cloud Application properties	14
Configuring InsuBiz Cloud Application user assignment.....	15

App description

The InsuBiz Cloud – MS 365 integration (*IB MS365 App*) is used to enable users to send e-mails directly from the InsuBiz Cloud platform using their own MS 365 mailbox or any shared mailbox they have permission to use.

E-mails sent this way, will be journalized in the InsuBiz Cloud solution and will be present in the users Outlook “Sent Items”.



Authentication

The *IB MS365 App* uses Microsoft Authentication Library (MSAL) to authenticate users and access Microsoft Graph API.

More information about MSAL can be found [here](#)

Security and permissions

The *IB MS365 App* is tenant and user aware.

All permissions required for the *IB MS365 App* are delegated permissions, meaning that the application needs an authorized user login to perform actions on behalf of this user and only the specific user that has been authorized.

The *IB MS365 App* cannot perform actions on behalf of the tenant.

Required permissions

Microsoft Graph			
User.Read	Sign in and read user profile	Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.	Used by InsuBiz Cloud to read basic information used for e-mail purposes.
Mail.Send	Send mail as a user	Allows the app to send mail as users in the organization.	Used by InsuBiz Cloud to send e-mails from the specific user's mailbox.
Mail.Send.Shared	Send mail on behalf of others	Allows the app to send mail as the signed-in user, including sending on-behalf of others	Used by InsuBiz Cloud to send e-mails from shared mailboxes that the specific user has access to.
openid	Sign users in	Allows users to sign in to the app with their work or school accounts and allows the app to see basic user profile information.	Used by InsuBiz Cloud to identify the specific user, and to ensure that the user is authorized. <i>(Standard in MSAL)*</i>
profile	View users' basic profile	Allows the app to see your users' basic profile (e.g., name, picture, user name, email address)	Used in the sign-in process to read needed user profile information <i>(Standard in MSAL) *</i>
offline_access	Maintain access to data you have given it access to	Allows the app to see and update the data you gave it access to, even when users are not currently using the app. This does not give the app any additional permissions.	Used by InsuBiz Cloud to be able to request refresh tokens from AAD <i>(Standard in MSAL) *</i>

* These permissions are required by MSAL

Permission details

Sign in and read user profile

Resource application ⓘ

Microsoft Graph

Claim value ⓘ

User.Read

Permission display name ⓘ

Sign in and read user profile

Permission description ⓘ

Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.

Permission type ⓘ

Delegated. Delegated type means that this application may act on behalf of a user as the user him or herself for this particular permission.

Send mail as a user

Resource application ⓘ

Microsoft Graph

Claim value ⓘ

Mail.Send

Permission display name ⓘ

Send mail as a user

Permission description ⓘ

Allows the app to send mail as users in the organization.

Permission type ⓘ

Delegated. Delegated type means that this application may act on behalf of a user as the user him or herself for this particular permission.

Send mail on behalf of others

Resource application ⓘ

Microsoft Graph

Claim value ⓘ

Mail.Send.Shared

Permission display name ⓘ

Send mail on behalf of others

Permission description ⓘ

Allows the app to send mail as the signed-in user, including sending on-behalf of others.

Permission type ⓘ

Delegated. Delegated type means that this application may act on behalf of a user as the user him or herself for this particular permission.

Sign users in

Resource application [\(i\)](#)

Microsoft Graph

Claim value [\(i\)](#)

openid

Permission display name [\(i\)](#)

Sign users in

Permission description [\(i\)](#)

Allows users to sign in to the app with their work or school accounts and allows the app to see basic user profile information.

Permission type [\(i\)](#)

Delegated. Delegated type means that this application may act on behalf of a user as the user him or herself for this particular permission.

View users' basic profile

Resource application [\(i\)](#)

Microsoft Graph

Claim value [\(i\)](#)

profile

Permission display name [\(i\)](#)

View users' basic profile

Permission description [\(i\)](#)

Allows the app to see your users' basic profile (e.g., name, picture, user name, email address)

Permission type [\(i\)](#)

Delegated. Delegated type means that this application may act on behalf of a user as the user him or herself for this particular permission.

Maintain access to data you have given it access to

Resource application [\(i\)](#)

Microsoft Graph

Claim value [\(i\)](#)

offline_access

Permission display name [\(i\)](#)

Maintain access to data you have given it access to

Permission description [\(i\)](#)

Allows the app to see and update the data you gave it access to, even when users are not currently using the app. This does not give the app any additional permissions.

Permission type [\(i\)](#)

Delegated. Delegated type means that this application may act on behalf of a user as the user him or herself for this particular permission.

Permission approval and admin consent

It is assumed, that the organization does not allow user consent to applications. Therefor an admin consent will be necessary to allow the users to access the InsuBiz Cloud – MS 365 integration.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo and a search bar that says "Search resources, services, and docs (G+/)". Below the header, the URL "Home > Contoso | Enterprise applications > Enterprise applications | Consent and permissions >" is visible. The main title is "Consent and permissions | User consent settings". On the left, a sidebar titled "Manage" lists three options: "User consent settings" (selected), "Admin consent settings", and "Permission classifications". The "User consent settings" section contains a description about controlling user consent for applications. It includes a heading "User consent for applications" and a sub-section "Configure whether users are allowed to consent for applications to access your organization's data. [Learn more](#)". Underneath, there are three radio button options: "Do not allow user consent" (selected, highlighted with a yellow box), "Allow user consent for apps from verified publishers, for selected permissions (Recommended)", and "Allow user consent for apps". A large orange callout bubble points to the "User Consent is not allowed" text in the description area.

Entra Id – Enterprise Applications

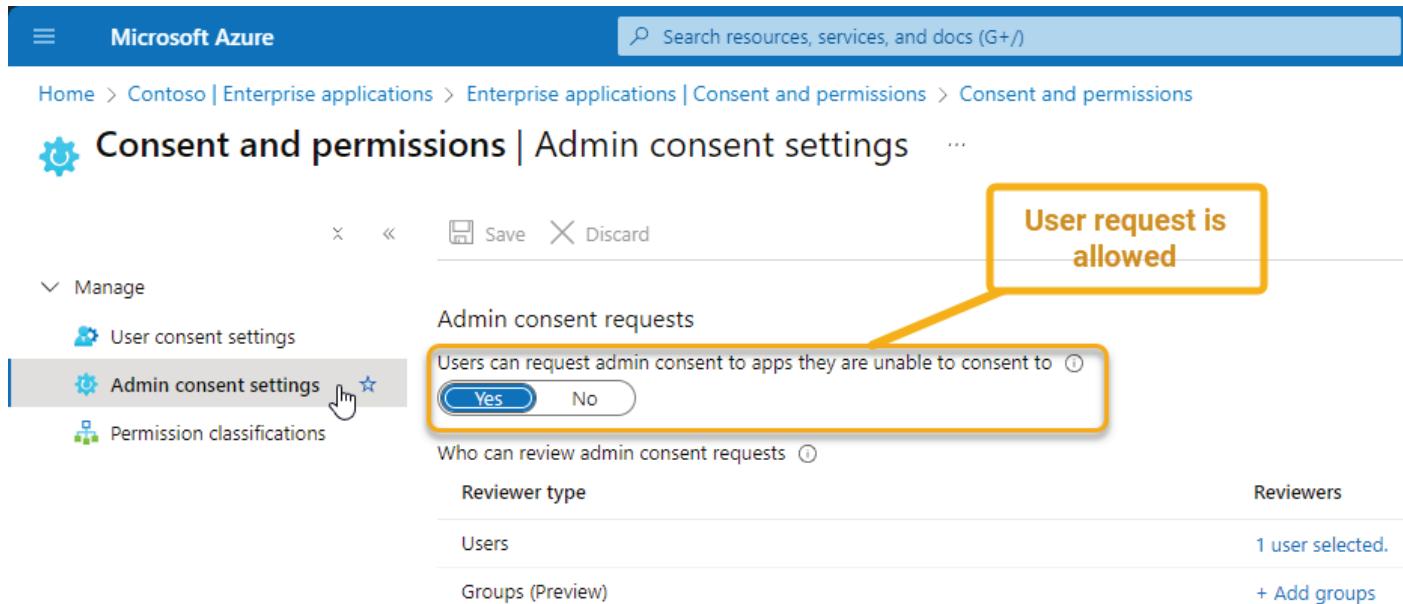
There are two primary methods for setting up the admin consent:

- Admin consent after user request.
- Admin consent using MS identity platform URL.

Both will be covered in the following.

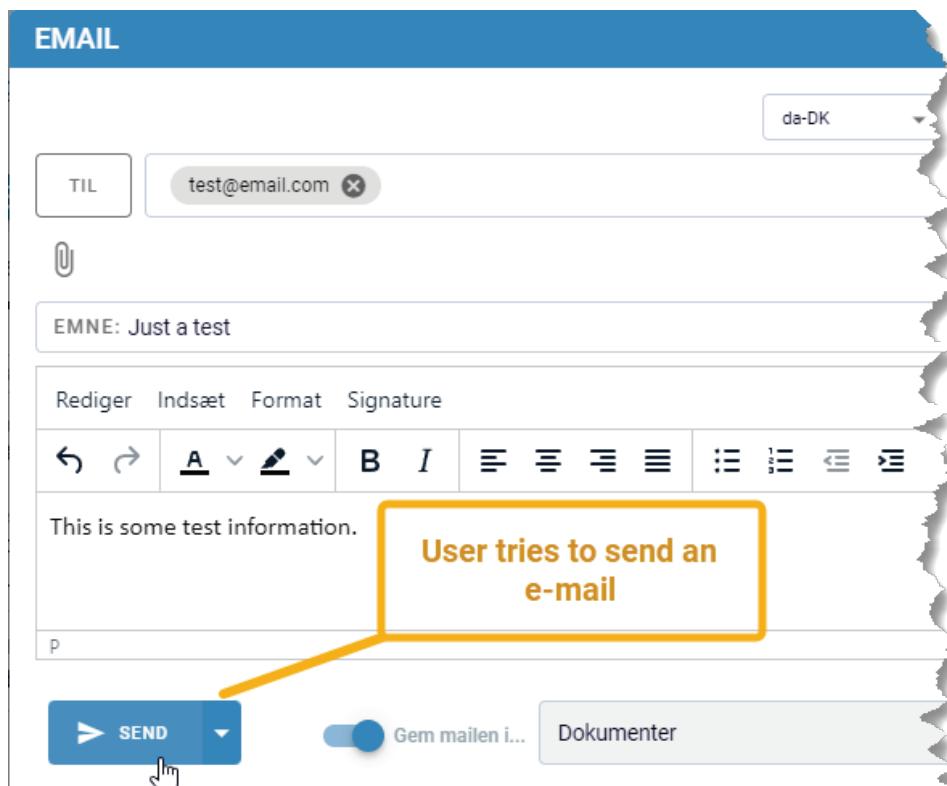
Admin consent after user request

When a user tries to use the e-mail integration functionality in InsuBiz Cloud, the system checks for the required permissions. If the permissions are not granted and users are allowed to request Admin Consent in the organization (see illustration below), the user can make a request for admin consent.



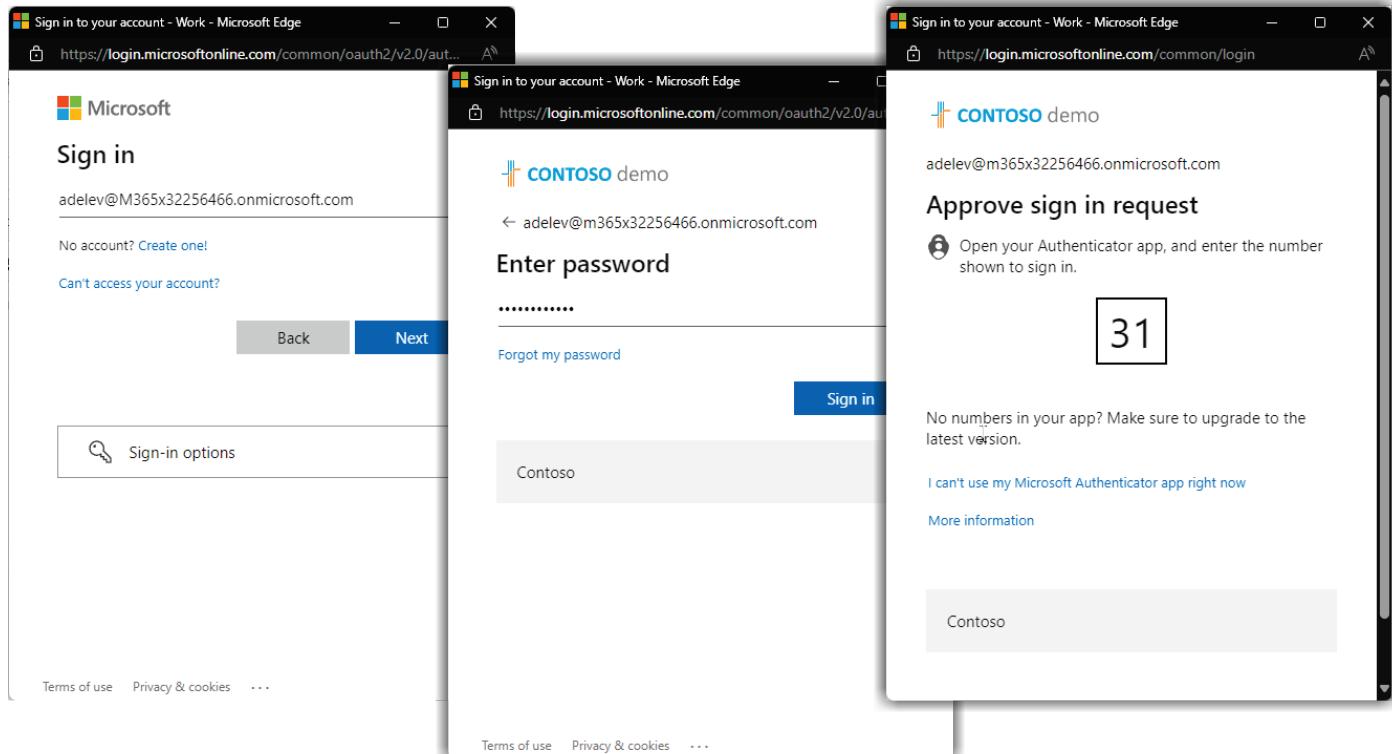
The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure', a search bar, and a breadcrumb trail: Home > Contoso | Enterprise applications > Enterprise applications | Consent and permissions > Consent and permissions. The main content area is titled 'Consent and permissions | Admin consent settings'. On the left, there's a sidebar with 'Manage' options: User consent settings, Admin consent settings (which is selected and highlighted with a blue border and a hand cursor icon), and Permission classifications. The main content area has a section titled 'Admin consent requests' with the sub-section 'Users can request admin consent to apps they are unable to consent to'. This section contains a button with 'Yes' (highlighted with a yellow box) and 'No'. A callout bubble points to this button with the text 'User request is allowed'. Below this, there's a section titled 'Who can review admin consent requests' with 'Reviewer type' set to 'Users' and 'Reviewers' listed as '1 user selected.' with a '+ Add groups' link. There are also tabs for 'Groups (Preview)'.

1 User tries to send an e-mail from the InsuBiz Cloud platform

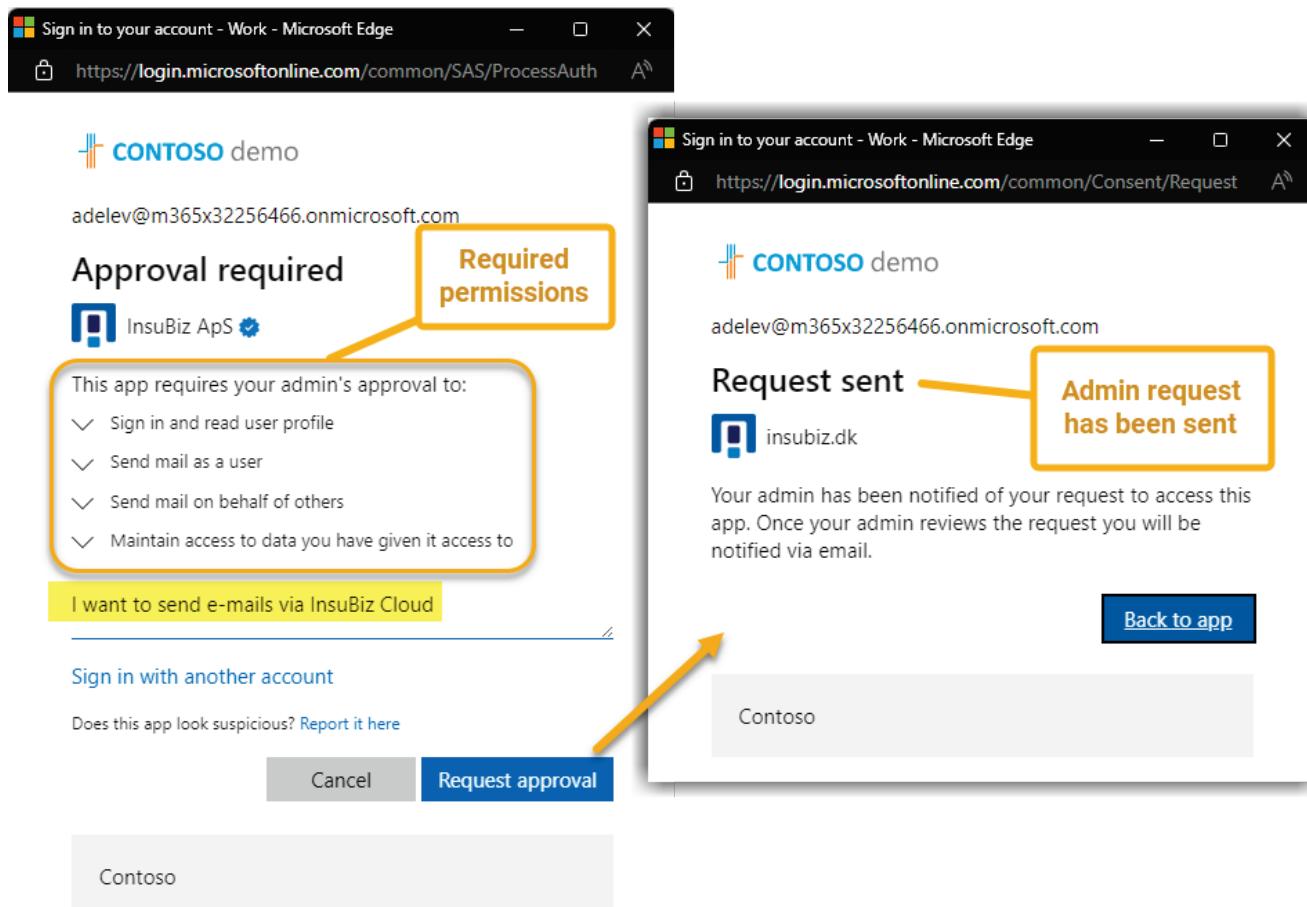


The screenshot shows the InsuBiz Cloud email interface. The top bar is blue with the word 'EMAIL'. The main area shows an email being composed to 'test@email.com'. The body of the email contains the text 'EMNE: Just a test' and 'This is some test information.'. A callout bubble points to this text with the text 'User tries to send an e-mail'. At the bottom, there's a toolbar with icons for Rediger, Indsæt, Format, and Signature. Below the toolbar, there's a rich text editor toolbar with buttons for backspace, forward, bold, italic, etc. At the bottom right, there's a 'SEND' button with a hand cursor icon, a 'Gem mailen i...' button, and a 'Dokumenter' button.

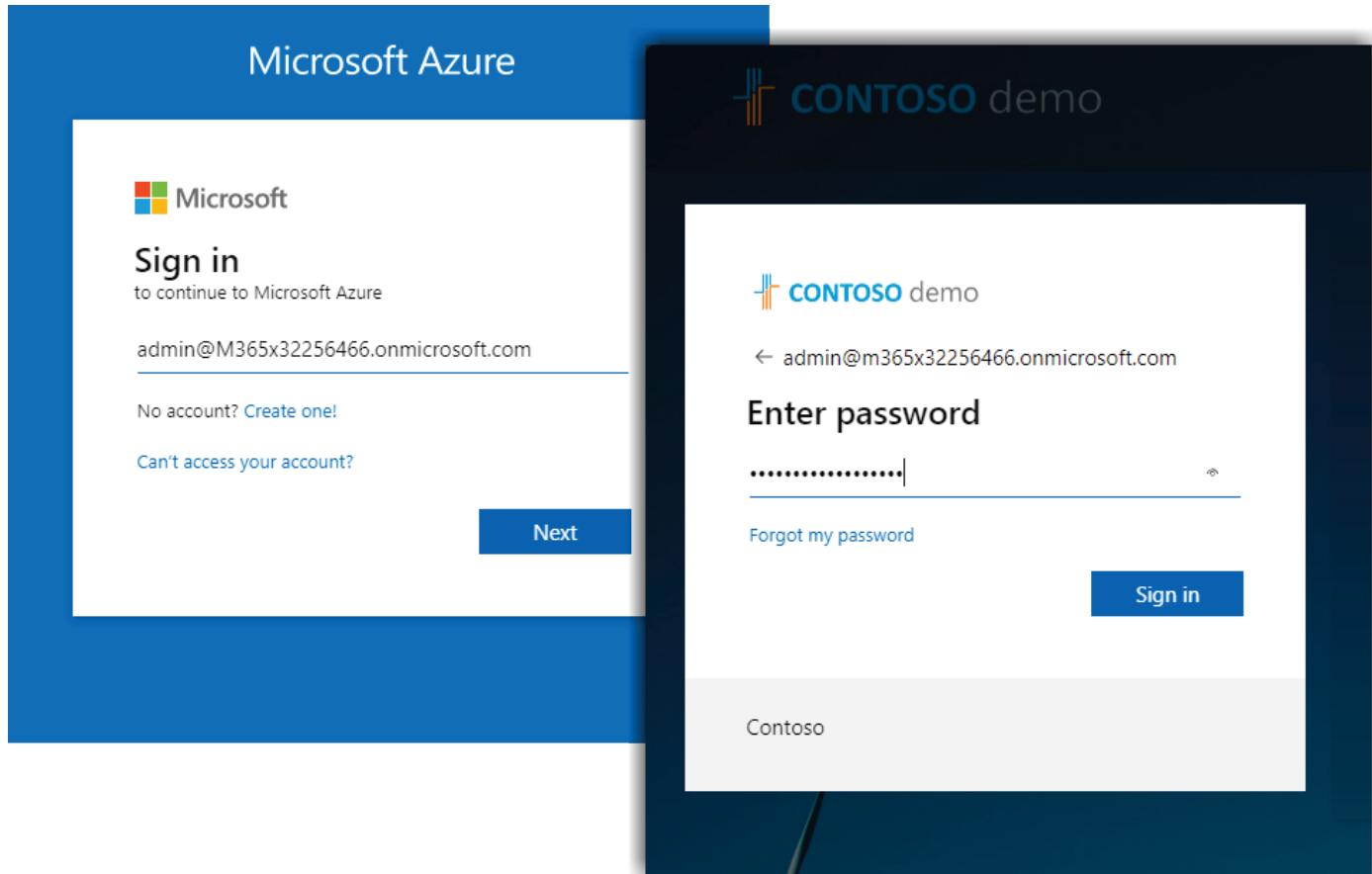
2 User is asked to sign in to their MS 365 account



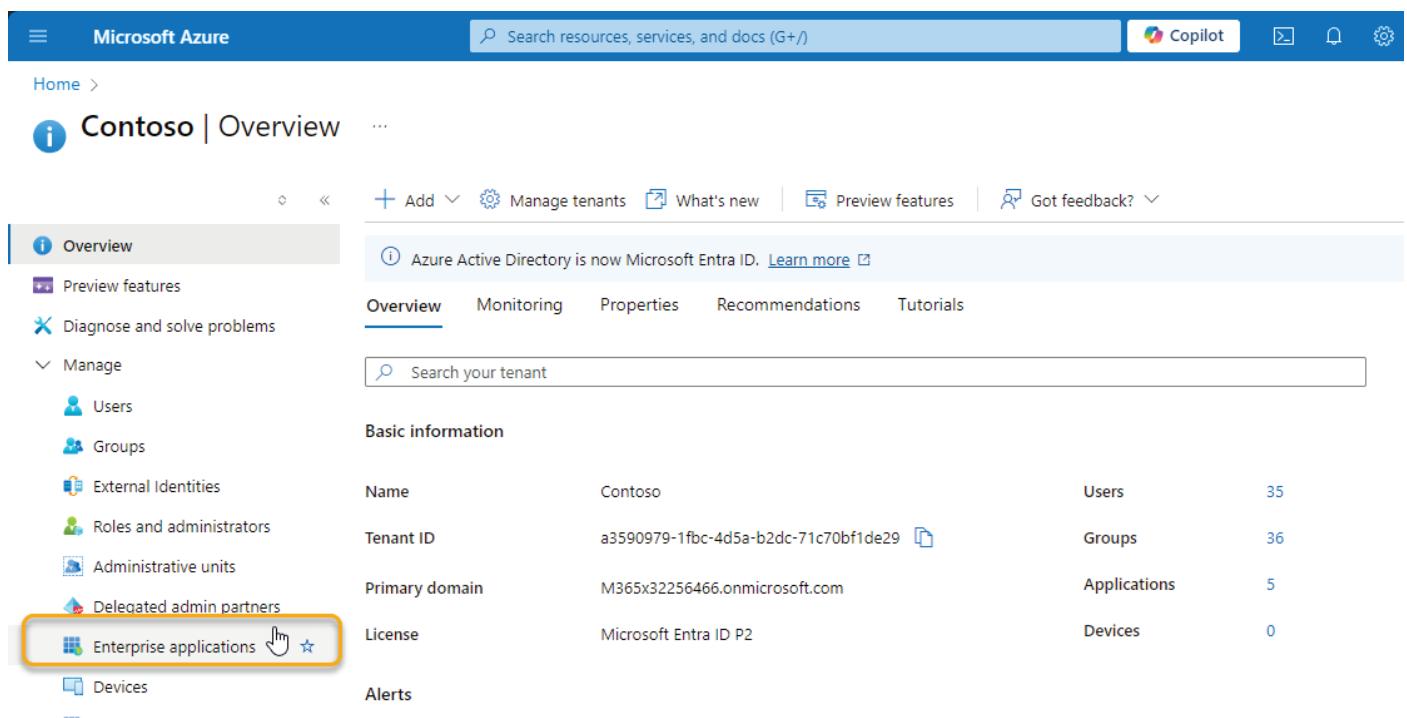
3 Approval is required, and the user can send an admin request



4 Sign in as Azure administrator on the organization



5 Go to Entra Id – Enterprise applications



Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Contoso | Overview

Add Manage tenants What's new Preview features Got feedback?

Overview

Azure Active Directory is now Microsoft Entra ID. [Learn more](#)

Manage tenants

Search your tenant

Basic information

	Name	Tenant ID	Primary domain	License	Users	Groups	Applications	Devices
Name	Contoso	a3590979-1fbc-4d5a-b2dc-71c70bf1de29	M365x32256466.onmicrosoft.com	Microsoft Entra ID P2	35	36	5	0

Enterprise applications

Devices

Alerts

6 Go to Enterprise applications – Admin consent requests

Screenshot of Microsoft Azure Enterprise applications Admin consent requests page:

- Left sidebar:** Overview, Manage, Security (Conditional Access, Consent and permissions), Activity (Sign-in logs, Usage & insights, Audit logs, Provisioning logs, Access reviews), Admin consent requests (highlighted with a yellow box), Bulk operation results.
- Header:** Microsoft Azure, Search resources, services, and docs (G+/-), Copilot, Refresh, Got feedback?
- Section:** My Pending All (Preview)
- Description:** When users try to access an application but are unable to provide consent, they can send a request for admin approval. Admins can control which applications your organization approves. Configured reviewers will be able to evaluate their pending consent requests in the "My Pending" queue. Global administrators, Application administrators, Cloud application administrators, and Global readers will be able to see all pending, expired, and completed consent requests in the "All" queue. [Learn More](#).
- Table:** Shows a single pending request for "InsuBiz Cloud".

A yellow callout box points to the "InsuBiz Cloud" row in the table with the text: "A pending request is shown".

Note: In some cases, the request may be shown with the name "InsuBiz InSight".

7 Click on the "InsuBiz Cloud" admin consent request

Open the request, revise the requested permissions and accept the request.

Details

Screenshots showing the process of accepting the admin consent request:

- Step 1:** Click on the "Review permissions and consent" link in the "Details" section of the admin consent request page.
- Step 2:** "Pick an account" dialog box is displayed, showing the user "MOD Administrator" signed in.
- Step 3:** "Permissions requested" dialog box is displayed, listing the following permissions:
 - Sign in and read user profile
 - Send mail as a user
 - Send mail on behalf of others
 - Maintain access to data you have given it access to
- Step 4:** The "Accept" button is highlighted with a yellow box.

InsuBiz Cloud will now be added as an Enterprise Application in the organization with the required permissions.

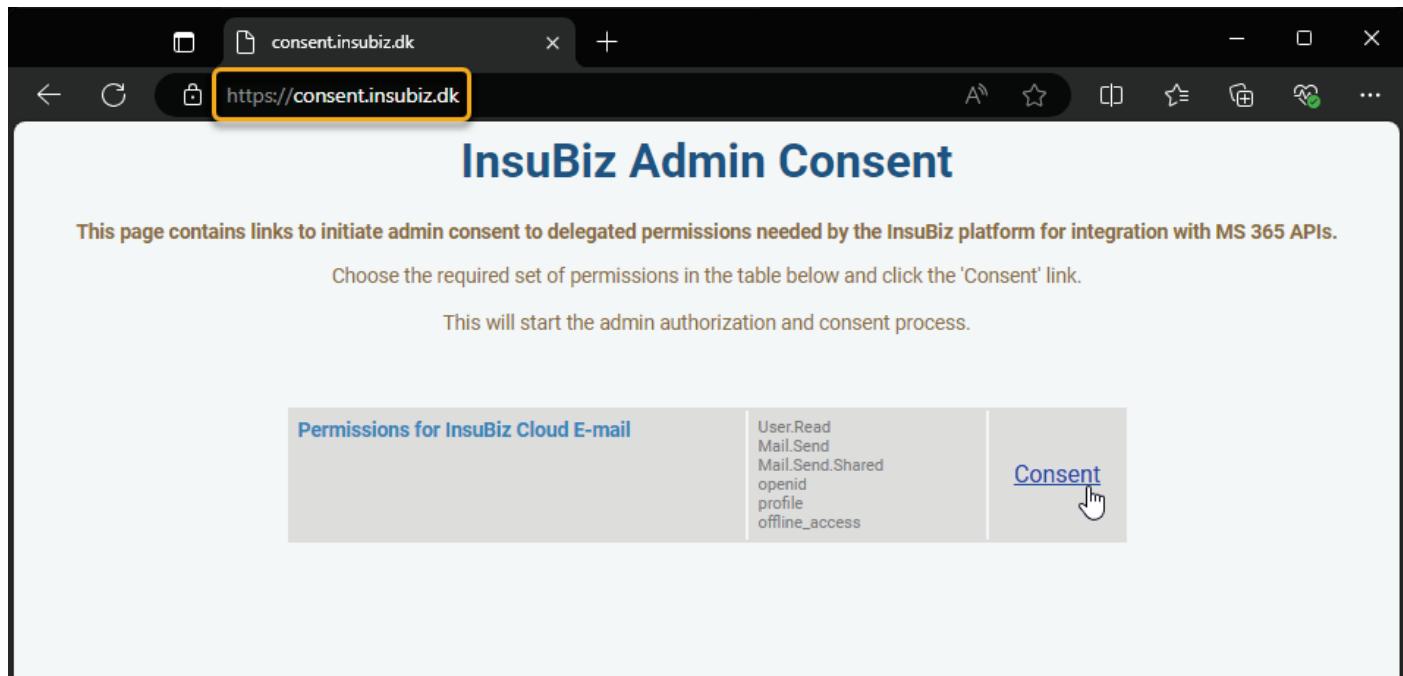
Admin consent using MS identity platform URL

It is possible to make an admin consent without a user request, by using the MS identity platform.

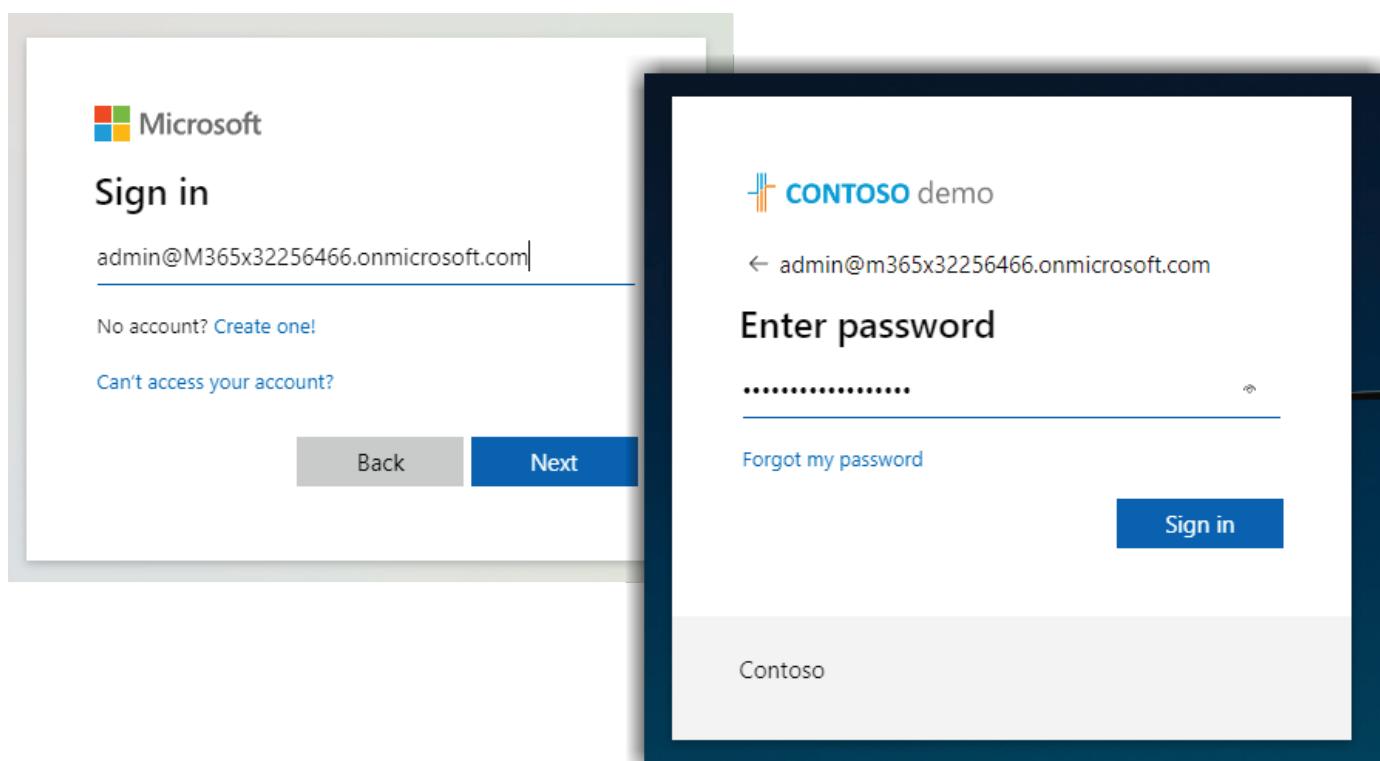
- 1 Go to the InsuBiz consent page to initiate the admin consent process

[**>> Start admin consent here <<**](#)

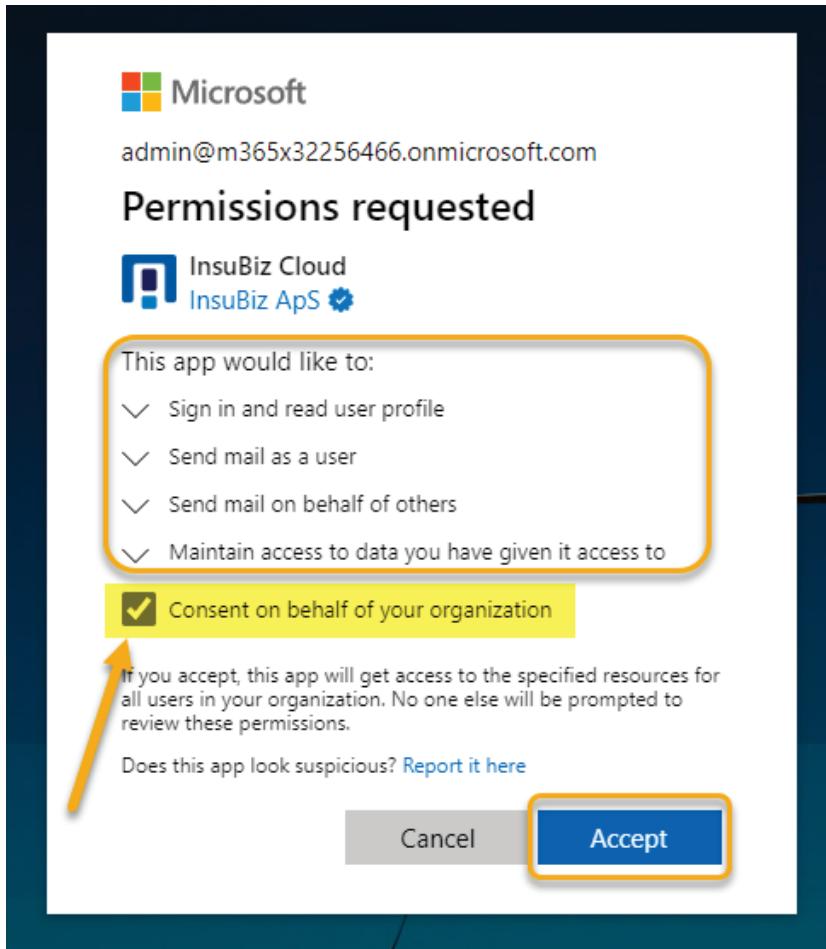
- 2 Click the "Consent" link for the required set of permissions



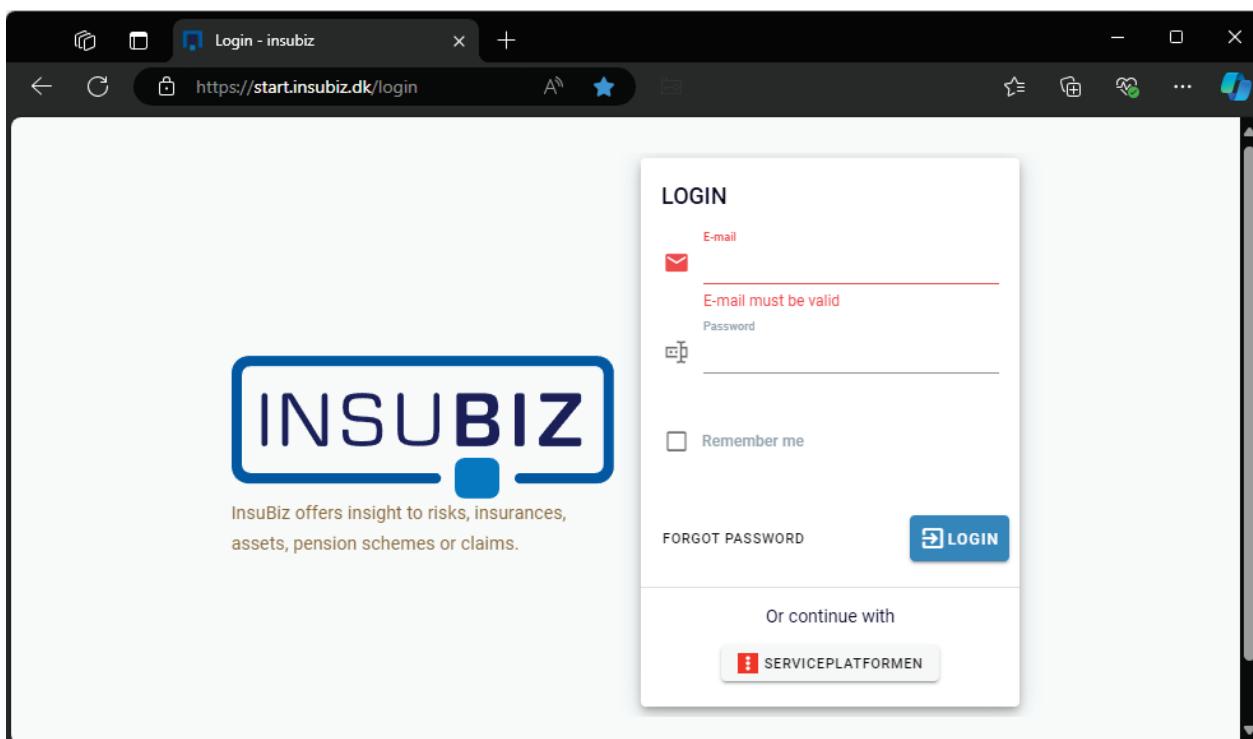
- 3 Sign in to an administrative account



4 Review requested permissions, make the consent on behalf of the organization and accept



5 The consent has been registered, and you are directed to the InsuBiz Cloud login page



This page can just be closed, since the consent process has been completed.

Review the permissions in the Enterprise Application

1 Select the InsuBiz Cloud Enterprise Application

The screenshot shows the Microsoft Azure portal interface. In the top navigation bar, 'Microsoft Azure' is selected. Below it, the breadcrumb path is 'Home > Contoso | Enterprise applications > Enterprise applications'. The main title is 'Enterprise applications | All applications'. On the left, a sidebar menu includes 'Overview', 'Manage' (with 'All applications' selected), 'Private Network connectors', 'User settings', 'Security' (with 'Conditional Access' and 'Consent and permissions' listed), 'Activity', and 'Sign-in logs'. The main content area displays a table of applications. A search bar at the top right says 'Search by application name or object ID' and 'Application type == Enterprise Applications'. The table has columns: Name, Object ID, Application ID, and Homepage URL. There are 9 applications found. One row, 'InsuBiz Cloud', is highlighted with a yellow box. The table data is as follows:

Name	Object ID	Application ID	Homepage URL
ProvisioningH...	51bfd075-61c0-4b72...	b6a9a780-a4a1-4955...	
BrowserStack	5a98d60b-ff81-466f...	187264c5-a2ad-4b09...	https://login.browser...
LinkedIn	75198162-f415-4b3f...	80e4af3d-0dd8-4648...	https://account.activ...
InsuBiz Cloud	9cdb978f-674a-4814...	348a93c9-caff-4c6e...	https://www.insubiz.dk
ProvisioningP...	abbad5d5-fa9d-4ddb...	ea708463-7f80-4331...	

2 Review the consented permissions

The screenshot shows the Microsoft Azure portal interface. In the top navigation bar, 'Microsoft Azure' is selected. Below it, the breadcrumb path is 'Home > Contoso | Enterprise applications > Enterprise applications | All applications > InsuBiz Cloud'. The main title is 'InsuBiz Cloud | Permissions'. On the left, a sidebar menu includes 'Deployment Plan', 'Diagnose and solve problems', 'Manage' (with 'Conditional Access' and 'Permissions' listed), 'Token encryption', 'Activity', and 'Troubleshooting + Support'. The 'Permissions' item is highlighted with a yellow box. The main content area displays a table of permissions under the heading 'Permissions'. A blue button at the top says 'Grant admin consent for Contoso'. The table has tabs for 'Admin consent' and 'User consent', with 'Admin consent' selected. A search bar at the top right says 'Search permissions'. The table data is as follows:

API Name	Claim value	Permission	Type
Microsoft Graph	User.Read	Sign in and read user profile	Delegated
Microsoft Graph	Mail.Send	Send mail as a user	Delegated
Microsoft Graph	Mail.Send.Shared	Send mail on behalf of others	Delegated
Microsoft Graph	openid	Sign users in	Delegated
Microsoft Graph	profile	View users' basic profile	Delegated
Microsoft Graph	offline_access	Maintain access to data you have given it...	Delegated

Configuring the InsuBiz Cloud Application properties

1 Select the InsuBiz Cloud Enterprise Application and select the 'Properties' tab

Microsoft Azure Search resources, services, and docs (G+ /) Copilot

Home > Contoso | Enterprise applications > Enterprise applications | All applications > InsuBiz Cloud

InsuBiz Cloud | Properties Enterprise Application

Save Discard Delete Got feedback?

Overview View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. [Learn more.](#)

Deployment Plan

Diagnose and solve problems

Manage

- Properties** (selected)
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Self-service
- Custom security attributes

Enabled for users to sign-in? Yes No

Name InsuBiz Cloud

Homepage URL <https://www.insubiz.dk>

Logo

Application ID 348a93c9-caff-4c6e-9f5e-58f89baad72d

Object ID 9cdb978f-674a-4814-a557-974cf49f7532

Assignment required? Yes No

Visible to users? Yes No

Optional

Recommended

It is recommended to select 'No' for the property "Visible to users". By doing that, the application will not be visible in the user's app palette.

It is possible to narrow the access to the application further by selecting 'Yes' for the property "Assignment required". By doing this, specific users or groups must be assigned to the application to access it. (See next section)

Configuring InsuBiz Cloud Application user assignment

If the “Assignment required” property is set to ‘Yes’, users must be assigned to the application either directly or via a group membership to access the integration functionality in InsuBiz Cloud.

- 1 Select InsuBiz Cloud enterprise application, select the “Users and groups” tab and click +Add...

The screenshot shows the Microsoft Azure portal interface for managing enterprise applications. The top navigation bar includes 'Microsoft Azure', a search bar, and a breadcrumb trail: Home > Contoso | Enterprise applications > Enterprise applications | All applications > InsuBiz Cloud. The main page title is 'InsuBiz Cloud | Users and groups'. On the left, there's a sidebar with links like Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Roles and administrators), and 'Users and groups' (which is highlighted with a yellow box and a hand cursor icon). At the top right, there are buttons for '+ Add user/group' (highlighted with a yellow box and a yellow arrow pointing from the 'Users and groups' link), Edit assignment, Remove, Update credentials, and Columns. A tooltip for '+ Add user/group' says: 'The application will not appear for assigned users within My Apps. Set 'visible to users?' to yes in properties to enable this.' Below this, there's a search bar with the placeholder 'First 200 shown, to search all users & group'. A table lists a single user entry: 'Display Name' (MA) and 'Object Type' (User). The 'MOD Administrator' role is indicated by a purple circle with 'MA'.

- 2 Click the link under “Users and groups”

The screenshot shows the 'Add Assignment' page for the InsuBiz Cloud application. The top navigation bar is identical to the previous screenshot. The main title is 'Add Assignment'. The left sidebar shows 'Contoso' and the 'Users and groups' section, which is highlighted with a yellow box and a hand cursor icon. Inside this section, there's a link 'None Selected' with a hand cursor icon, and below it, a link 'Select a role' with a hand cursor icon. At the bottom of this section is a link 'Default Access'. At the very bottom of the page is a large 'Assign' button.

3 Check all necessary users and groups and click "Select"

The screenshot shows the 'Users and groups' search interface in Microsoft Azure. A user named 'Adele Vance' is selected and highlighted with a yellow box. An arrow points from the 'Select' button at the bottom to the selected user.

Name	Type
Adele Vance	User
All Company	Group

4 Click "Assign"

The screenshot shows the 'Add Assignment' page in Microsoft Azure. The 'Assign' button is highlighted with a yellow box.

5 The users and group shas now been assigned to the Application

The screenshot shows the 'InsuBiz Cloud | Users and groups' page in Microsoft Azure. The user 'Adele Vance' is highlighted with a yellow box.

Display Name	Object Type
MOD Administrator	User
Adele Vance	User